Licence professionnelle *Réseaux et Sécurité*
Projets tuteurés 2014-2015

Sujets proposés à l'Université de Cergy-Pontoise

1. Déploiement d'une architecture téléphonique hybride : PC-Asterisk/PABX analogique + annuaire et proxy (3 élèves)

Tuteur : *Tuyêt Trâm Dang Ngoc***,** dntt(à)u-cergy.fr

Le but de ce projet est de déployer la téléphonie sur IP et analogique sur un site puis de l'interconnecter avec un autre site.

a. Site 1

Création d'un autocommutateur analogique

Vous disposez d'un PC contenant les deux cartes suivantes Digium TDM31B TDM PCI Card (3FXS-1FXO). Sur chacune de ces cartes, vous pouvez relier sur les ports FXS, un périphérique analogique FXO (téléphone, fax, etc.) et sur les ports FXO une liaison vers un port FXS.
Le logiciel Asterisk permet de transformer un tel PC en un autocommutateur PABX. Dans cette première étape, vous créerez un autocommutateur sur ce PC.
Pour cela :

- Vous installerez et configurerez Asterisk afin de prendre en charge les ports FXS.
- Vous attribuerez à votre autocommutateur le préfixe 0123 et vous numéroterez les ports FXS 1000, 1001, 1002, 1003, etc.
- Vous disposez de téléphones analogiques pour tester votre autocommutateur. Connectez vos téléphones et composez le numéro de téléphone depuis un téléphone vers un autre pour tester le bon fonctionnement de votre autocommutateur.
- Faites en sorte qu'il puisse y avoir affichage du numéro et transfert d'appel.

Création d'un réseau téléphonique IP

Vous disposez d'un autre PC ne possédant pas de cartes dédiées à la téléphonie (pas de FXS ou FXO), simplement une carte réseau Ethernet. Il s'agit ici de réaliser un PBX entièrement basé sur IP. La téléphonie sur IP s'appuie sur le protocole SIP.

- Vous mettrez en place le réseau 192.168.42.0/24 sur lequel vous connecterez votre PBX IP ainsi que deux autres PC.
- Vous créerez des lignes SIP 2000, 2001, 2002, etc. que vous attribuerez aux téléphones IP. Vous utiliserez plusieurs types de téléphones IP : un téléphone IP filaire, un téléphone IP wifi, un softphone comme ekiga + casque et micro, un téléphone USB
- Connectez vos téléphones et composez le numéro de téléphone depuis un téléphone vers un autre pour tester le bon fonctionnement de votre autocommutateur IP.
- Faites en sorte qu'il puisse y avoir affichage du numéro et transfert d'appel.
- Mettez en place et expérimentez au maximum les services offerts par Asterisk : présentation du nom, filtrage d'appel, etc.

Création de la passerelle analogique

- Reliez votre PC commutateur analogique au réseau IP construit dans la section précédente.
- Faites en sorte que les téléphones IP puissent appeler les téléphones analogiques du réseau RTC et vice-versa.

b. Site 2

Créez un deuxième site identique au premier puis réalisez l'interconnexion afin de permettre la téléphonie entre les deux sites.

c. Fonctionnalités supplémentaires

- Utilisation de proxy et de redirecteur pour la téléphonie IP : Mettez en place un proxy et un redirecteur permettant l'enregistrement des numéros et (jabber) téléphone dans un intranet. Cette fonctionnalité est importante par rapport à l'évaluation finale du projet.
- Intégration LDAP : Vous déploierez et utiliserez un annuaire LDAP pour les services de présentation du nom, recherche numéro, etc.
- Visio-conférence: Sur votre machine Asterisk, prenez en compte le protocole H323 afin de permettre la visio-conférence. Testez.

Travail demandé

Vous répondrez à toutes les exigences demandées en déployant soigneusement votre plateforme téléphonique qui devra être fonctionnelle, maintenable et redéployable. Une attention particulière sera donnée à l'élaboration du rapport technique devant décrire les architectures manipulées, les pré-requis et les concepts notamment de téléphonie ainsi que les difficultés rencontrées, les remarques et les limitations. Le manuel d'installation et la description des configurations de logiciels seront quant à eux donnés en annexe.

2. Gestionnaire de parc informatique (2 élèves)

Tuteur : *Tuyêt Trâm Dang Ngoc***,** dntt(à)u-cergy.fr

Le contexte

GLPI (gestionnaire libre de parc informatique) est une application web permettant la gestion de parc informatique et de gestion des services d'assistance. Il est utilisé par de nombreuses entreprises.

OCS Inventory NG est une application permettant de réaliser un inventaire sur la configuration matérielle des machines du réseau et sur les logiciels qui y sont installés et de visualiser ces informations grâce à une interface web. Il peut être utilisé pour alimenter GLPI.

Ces services web permettent d'extraire les données, offrent des services de suivi d'historique (effacement, fusion...) et donnent la possibilité de paramétrer le fonctionnement de l'application.

Enfin, GLPI possède de nombreux plugins permettant de réaliser l'inventaire du matériel (par saisie manuelle, code-barre, découverte), cartographier le matériel et le réseau, de gérer les commandes et les tickets d'assistance, etc.

De nombreuses entreprises utilisent GLPI/OCS afin de rationaliser leurs ressources.

Votre travail

Vous devez réaliser une plate-forme de démonstration des possibilités de GLPI/OCS. Pour cela, vous aurez à gérer :

- Un exemple de stock de matériel informatique (PC, serveurs, équipement réseaux)
- Un exemple de stock de logiciels, licences, etc.
- Un exemple de stock de mobilier non connecté (voir l'utilisation de codes-barres)
- Du matériel connecté en réseau

Dans ce cadre, vous devrez mettre en place un système d'inventaire, de gestion de ticket, de cartographie et de remontée/mise à jour automatique.

Vous devrez également prévoir des scénarios de tests pertinents pour mettre en évidence les fonctionnalités que vous voulez montrer mais aussi leurs limites.

Enfin, une documentation précise devra être délivrée.

3. Benchmark de virtualisation (2-3 élèves)

Tuteur : *Guillaume Renier***,** guillaume.renier(à)u-cergy.fr

Objet
Comparaison de solution de virtualisations. Comparaison de systèmes de stockage partagé en situation de virtualisation.

Les tests et les protocoles de tests seront décidés avec les étudiants.
Le choix de ces tests, méthodes, protocoles fait partie du sujet.
Le sujet peut se résumer par la question : "Virtualiser pourquoi, pourquoi pas ?"

Matériel disponible :

- serveurs DELL R410, R510, R710. NAS.
- Baie de virtualisation VMware avec ESX et HA.
- Switchs, routeurs, tous logiciels UNIX et Microsoft.

Possibilité de tests de DB MSSQL en mode miroir, cluster de basculement pour benchmark.

4. Haute disponibilité et répartition de charge en environnement web (2 élèves)

Tuteur : *Marc Lemaire***,** marc.lemaire(à)u-cergy.fr

Contexte

L'objectif de ce projet est la réalisation d'un prototype d'une infrastructure web (serveurs Apache et MySQL) en haute disponibilité (redondance et répartition de charge) en environnement Unix / Linux.

Serveurs Web

La ressource web sera constituée de 3 serveurs web apache2 (l'accès sera balancé via un seul point d'entrée ou en mode routage direct). La gestion de ce premier cluster pourra s'appuyer sur une solution de type « pacemaker » (en explorant si possible les alternatives « heartbeat » et « corosync ») ou éventuellement une solution équivalente.

Plusieurs critères devront idéalement être respectés : redondance du stockage et synchronisation des fichiers sur les 3 serveurs web (en exploitant les possibilités de « rsync » par exemple), répartition de charges (« load balancing ») avec un test de simulation de montée en charge, haute disponibilité (« High Availability ») en testant les différentes situations de panne (réseau / matériel / processus / système) puis de reprise.

Serveurs de bases de données

Pour la partie base de données, il est demandé d'explorer la solution « MySQL Cluster » avec un minimum de 3 nœuds. Sachant que les bases actuellement utilisées s'appuient sur les moteurs de stockage InnoDB et MyISAM, une analyse des conséquences de l'utilisation du moteur de stockage NDB imposé par cette solution serait souhaitable.

Les mêmes contraintes de haute disponibilité et de répartition de charge sont attendues pour cette seconde partie.

Sujets proposés à l'EPMI

5. Architecture réseau (2-3 élèves)

Tuteurs *Nabil Ouassini,* n.ouassini(à)epmi.fr, *Jean DOS SANTOS,* j.dossantos(à)epmi.fr

L'entreprise HYDROGEOL rencontre des problèmes avec son ancienne installation réseau, elle avait beaucoup de difficultés à assurer la continuité du service avec son fournisseur d'accès.

Après étude, la direction a décidé de faire quelques modifications à son architecture réseau.

La solution est de mettre en place un AD avec un serveur DNS, DHCP et un serveur RADIUS sous Windows 2008 R2 pour une authentification unique, ainsi que des bornes WIFI pour ses clients, plus un firewall de type IPFIRE ou PFSENSE. Deux abonnements internet chez deux fournisseurs d'accès différents sont prévus, pour assurer la continuité de service, avec une redondance au niveau des routeurs, en mettant en place un des protocoles suivants : HSRP, GLBP ou VRRP, avec une surveillance de l'adresse IP des deux fournisseurs d'accès pour éviter tout déconnection.

Votre mission est de mettre en place cette architecture, faire une comparaison entre les 3protocoles et donner des explications sur votre choix.

Pour les clients wifi mettre en place des certificats pour sécuriser le réseau.

Les suggestions d'amélioration de cette architecture sont les bienvenues.

Matériel mis à disposition

- 2 router cisco
- 2 switch cisco
- 2 bornes WIFI
- 4 UC
- 1 router DLINK.

6. Sécurisation réseau (2-3 élèves)

Tuteurs *Nabil Ouassini,* n.ouassini(à)epmi.fr, *Jean DOS SANTOS,* j.dossantos(à)epmi.fr

Une entreprise souhaite sécuriser son réseau, dont l'architecture est décrite comme suit :

- Un réseau local avec l'adressage 192.168.1.0/24
- Un accès WAN avec l'@ IP de sortie 78.95.66.1
- Deux serveurs FTP et HTTP publics ayant des @ dans le réseau 10.1.1.0/24 (à placer dans une zone DMZ).

Les clients dans le réseau local sont autorisés à naviguer sur le web (le protocole http est autorisé dans le sens LAN_ WAN)

Parfois des clients distants doivent se connecter sur le réseau local pour faire des transactions sécurisées et ceci en utilisant une connexion à travers un VPN.

L'administrateur réseau doit accéder depuis la machine LAN vers la zone DMZ moyennant le protocole SSH.

L'authentification entre le serveur SSH et son client doit se faire avec des clés pass avec des mots de passes.

Travail demandé

- Reproduire l'architecture de réseau en utilisant des machines virtuelles sous Linux. On vous demande de faire la connectique physique nécessaire ainsi que la configuration du routage pour

tester la connectivité entre les trois zones (LAN, WAN et DMZ).

Vérifier la création d'un segment LAN différent pour chaque zone de la maquette.

- Etablir la politique de filtrage à adopter pour contrôler l'accès vers les différentes zones de cette maquette.
- Rendre le serveur http en HTTPS.
- Installer et configurer Pfsense comme firewall pour sécuriser l'accès à travers les différentes zones.
- Installer et configurer snort comme sonde IDS sur la machine LAN avec l'interface graphique BASE.
- Installer et configurer openvpn sur les deux machines LAN et WAN.

  Type du tunnel : ethernet tunnel. Sous réseau du tunnel VPN 172.16.10.0/24
- Installer et configurer openssh sur la machine DMZ et un client SSH sur la machine LAN et configurer une authentification par clé.

Matériel mis à disposition

- un serveur Dell power edge 411
- 3 UC
- 1 switch
- Des cartes réseau
- Une borne wifi

7. Supervision de réseau (2-3 élèves)

Tuteur *Nabil Ouassini,* n.ouassini(à)epmi.fr, *Jean DOS SANTOS,* j.dossantos(à)epmi.fr

Pour superviser son réseau, l'administrateur réseau d'une entreprise a décidé de mettre en place un outil de supervision avec une cartographie sous Nagios et nagvis. Le système utilisé centos.

Votre mission est de réaliser cette maquette en supervisant les équipements qui sont dans votre salle et rendre un rapport détaillé sur le projet, l'installation et les choix apportés.

Pour ce projet vous aurez à votre disposition :

- 2 switch
- 1 routeur
- 3 UC
- Une borne wifi
- Un routeur
- Logiciel Microsoft VISIO

8. Serveur de communication en temps réel (2-3 élèves)

Tuteur *Nabil Ouassini,* n.ouassini(à)epmi.fr, *Jean DOS SANTOS,* j.dossantos(à)epmi.fr

Notre école a décidé de mettre en place un serveur de communication en temps réel qui fournit l'infrastructure nécessaire à l'utilisation de la messagerie instantanée, la présence, de la voix et de la visio-conférence sous le système d'exploitation microsoft lync server 2013.

Votre mission est de réaliser cette installation.